



Department of Homeland Security Office of Inspector General

Information Technology Management Letter for the FY 2009 Immigration Customs Enforcement Financial Integrated Audit





Homeland
Security

May 18, 2010

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report presents the information technology (IT) management letter for the FY 2009 Immigration and Custom Enforcement (ICE) financial statement audit as of September 30, 2009. It contains observations and recommendations related to information technology internal control that were summarized in the *Independent Auditors' Report*, dated December 18, 2009 and presents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at ICE in support of the DHS FY 2009 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated April 1, 2010, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink, appearing to read "Frank Deffer".

Frank Deffer
Assistant Inspector General for
Information Technology Audits



KPMG LLP
2001 M Street, NW
Washington, DC 20036

April 1, 2010

Inspector General
U.S. Department of Homeland Security

Chief Information Officer and
Chief Financial Officer
Immigration and Customs Enforcement

Ladies and Gentlemen:

We have audited the consolidated balance sheet of the Immigration and Customs Enforcement (ICE), a component of the U.S. Department of Homeland Security (DHS), as of September 30, 2009 and the related consolidated statements of net cost, changes in net position, and the combined statement of budgetary resources (hereinafter referred to as “consolidated financial statements”) for the year then ended. In planning and performing our audit of the consolidated financial statements of ICE, in accordance with auditing standards generally accepted in the United States of America, we considered ICE’s internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements but not for the purpose of expressing an opinion on the effectiveness of ICE’s internal control. Accordingly, we do not express an opinion on the effectiveness of ICE’s internal control.

In planning and performing our fiscal year 2009 audit, we considered ICE’s internal control over financial reporting by obtaining an understanding of the design effectiveness of ICE’s internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls as a basis for designing our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements. To achieve this purpose, we did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers’ Financial Integrity Act of 1982*. The objective of our audit was not to express an opinion on the effectiveness of ICE’s internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of ICE’s internal control over financial reporting.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity’s financial statements will not be prevented, or detected and corrected on a timely basis.

Our audit of ICE as of, and for the year ended, September 30, 2009 disclosed a material weakness in the areas of information technology (IT) configuration management, security management, access controls, and segregation of duties. These matters are described in the *IT General Control Findings by Audit Area* section of this letter.



The material weakness described above is presented in our *Independent Auditors' Report*, dated December 18, 2009. This letter represents the separate restricted distribution letter mentioned in that report.

The control deficiencies described herein have been discussed with the appropriate members of management, and communicated through a Notice of Finding and Recommendation (NFR). Our audit procedures are designed primarily to enable us to form an opinion on the consolidated financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim to use our knowledge of ICE gained during our audit engagement to make comments and suggestions that are intended to improve internal control over financial reporting or result in other operating efficiencies.

The Table of Contents on the next page identifies each section of the letter. We have provided a description of key ICE financial systems and IT infrastructure within the scope of the FY 2009 ICE consolidated financial statement audit in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to certain additional matters have been presented in a separate letter to the Office of Inspector General and the ICE Chief Financial Officer dated December 9, 2009.

This communication is intended solely for the information and use of DHS and ICE management, DHS Office of Inspector General, OMB, U.S. Government Accountability Office, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

	Page
Objective, Scope and Approach	1
Summary of Findings and Recommendations	3
IT General Control Findings by Audit Area	4
Findings Contributing to a Material Weakness in IT	4
Configuration Management	4
Security Management (includes After-Hours Physical Security Testing)	4
Access Controls	5
Segregation of Duties	5
Application Controls	9
Management’s Comments and OIG Response	9

APPENDICES

Appendix	Subject	Page
A	Description of Key ICE Financial Systems and IT Infrastructure within the Scope of the FY 2009 DHS Financial Statement Audit Engagement	10
B	FY 2009 Notices of IT Findings and Recommendations at ICE	12
	- Notice of Findings and Recommendations – Definition of Severity Ratings	13
C	Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at ICE	19
D	Management’s Comments	21
E	Report Distribution	22

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

OBJECTIVE, SCOPE AND APPROACH

We have audited the Immigration and Custom Enforcement (ICE) agency's balance sheet as of September 30, 2009. In connection with our audit of ICE's balance sheet, we performed an evaluation of information technology general controls (ITGC), to assist in planning and performing our audit. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our ITGC evaluation procedures. The scope of the ITGC evaluation is further described in Appendix A.

FISCAM was designed to inform financial auditors about IT controls and related audit concerns to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial audit. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following five control functions to be essential to the effective operation of the general IT controls environment.

- *Security Management (SM)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Access Control (AC)* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.
- *Contingency Planning (CP)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our general IT controls audit procedures, we also performed technical security testing for key network and system devices, as well as testing over key financial application controls in the ICE environment. The technical security testing was performed both over the Internet and from within select ICE facilities, and focused on test, development, and production devices that directly support key general support systems.

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

In addition to testing ICE's general control environment, we performed application control tests on a limited number of ICE's financial systems and applications. The application control testing was performed to assess the controls that support the financial systems' internal controls over the input, processing, and output of financial data and transactions.

- *Application Controls (APC)* - Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2009, ICE took corrective action to address prior year IT control weaknesses. For example, ICE made improvements over tracking and maintaining Active Directory Exchange (ADEX) user access forms and securing its backup facility from unauthorized access. However, during FY 2009, we continued to identify IT general control weaknesses that could potentially impact ICE's financial data. The most significant weaknesses from a financial statement audit perspective related to controls over the Federal Financial Management System (FFMS) and the weaknesses over physical security and security awareness. Collectively, the IT control weaknesses limited ICE's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over ICE financial reporting and its operation and we consider them to collectively represent a material weakness for ICE under standards established by the American Institute of Certified Public Accountants (AICPA). In addition, based upon the results of our test work, we noted that ICE did not fully comply with the requirements of the *Federal Financial Management Improvement Act* (FFMIA).

Of the 14 findings identified during our FY 2009 testing, all were new IT findings. These findings represent weaknesses in four of the five FISCAM key control areas. Specifically these weaknesses are: 1) unverified access controls through the lack of comprehensive user access privilege re-certifications, 2) security management issues involving staff security training, exit processing procedures and contractor background investigation weaknesses, 3) inadequately designed and operating configuration management, and 4) lack of effective segregation of duties controls within financial applications. These weaknesses may increase the risk that the confidentiality, integrity, and availability of system controls and ICE financial data could be exploited thereby compromising the integrity of financial data used by management and reported in ICE's financial statements.

While the recommendations made by KPMG should be considered by ICE, it is the ultimate responsibility of ICE management to determine the most appropriate method(s) for addressing the weaknesses identified based on their system capabilities and available resources.

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

IT GENERAL CONTROL FINDINGS BY AUDIT AREA

Findings Contributing to a Material Weakness Deficiency in IT

During the FY 2009 financial statement audit, we identified the following IT and financial system control deficiencies that in the aggregate are considered a material deficiency:

1. Configuration Management – we identified:
 - Security configuration management weaknesses on ADEX. These weaknesses included default configuration settings, inadequate patches, and weak password management.

2. Security Management – we identified:
 - During social engineering testing, 5 out of 20 staff provided their login and password.
 - Physical security weaknesses which identified improper protection of system user names and passwords, unsecured information security hardware, documentation containing Personally Identifiable Information (PII) or marked “For Official Use Only”, and unlocked network sessions. The specific results are listed below:

Exceptions Noted	ICE Locations Tested			Total Exceptions by Type
	OFM TechWorld 10 th floor	OCIO PCN 3 rd floor	OCFO PCN 4 th floor	
User Name and Passwords	19	3	4	26
For Official Use Only (FOUO)	1	2	1	4
Keys/Badges	0	1	1	2
Personally Identifiable Information (PII)	13	2	0	15
Server Names/IP Addresses	0	2	0	2
Laptops	1	2	0	3
External Drives	2	3	1	6
Credit Cards	1	0	0	1
Classified Documents	0	0	0	0
Other - Describe	1 personal checkbook	1 workstation logged in w/o screensaver activated	1 workstation logged in w/o screensaver activated	3
Total Exceptions by Location	38	16	8	62

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

- Procedures for transferred and terminated personnel exit processing are not being consistently followed.
 - Background reinvestigations for contractors were not consistently performed.
 - IT Security training is not mandatory nor is compliance monitored.
3. Access controls – we identified:
- A lack of recertification of ADEX and FFMS system users.
 - ADEX account lockout settings are not compliant with DHS policy.
 - ADEX system access was not consistently removed for terminated employees and contractors.
 - FFMS password settings are not compliant with DHS policy.
 - Physical security personnel are not adequately trained to detect non-conforming credentials that can be used to gain unauthorized access.
4. Segregation of Duties – we identified:
- FFMS roles and responsibilities for the Originator, Funds Certification Official, and Approving Official profiles were not effectively segregated.

Recommendations: We recommend that the ICE Chief Information Officer (CIO) and Chief Financial Officer (CFO), in coordination with the DHS Office of Chief Financial Officer and the DHS Office of the Chief Information Officer, make the following improvements to ICE’s financial management systems and associated information technology security program.

Configuration Management:

1. Redistribute procedures and train employees on continuously monitoring and mitigating vulnerabilities. In addition, we recommend that ICE periodically monitor the existence of unnecessary services and protocols running on their servers and network devices, in addition to deploying patches.
2. Perform vulnerability assessments and penetration tests on all offices of the ICE, from a centrally managed location with a standardized reporting mechanism that allows for trending, on a regularly scheduled basis in accordance with NIST guidance.
3. Develop a more thorough approach to track and mitigate configuration management and resource vulnerabilities identified during monthly scans. ICE should monitor the vulnerability reports for necessary or required configuration changes to its environment.
4. Develop a process to verify that systems identified with “HIGH/MEDIUM Risk” configuration vulnerabilities do not appear on subsequent monthly vulnerability scan reports, unless they are verified and documented as a false-positive. All risks identified during the monthly scans should be mitigated immediately, and not be allowed to remain dormant.
5. Implement the corrective actions identified during the audit vulnerability assessment.

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

Security Management:

1. Ensure that users are trained and aware of safeguarding login credentials, locking network sessions to DHS systems, and locking any sensitive information, media containing sensitive information, or data not suitable for public dissemination in secure locations when not in use.
2. Effectively limit access to DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data to authorized personnel.
3. Adhere to exit clearance procedures and require personnel to follow them in the event of transfer\termination.
4. Periodically review personnel files to confirm background reinvestigations have been completed in accordance with DHS standards.
5. Implement mandatory requirements for IT security personnel to complete training consistent with their job function duties.
6. Remove system access for personnel that are not in compliance with training requirements. In addition, document procedures regarding disabling user accounts and access privileges in accordance with DHS policy.

Access Controls:

1. Establish and implement policies and procedures for recertification of system user privileges. This process should include a method to document user recertification and a process to maintain evidence of the reviews.
2. Develop processes for the removal of transferred and terminated users within ADEX upon their separation.
3. Modify ADEX lockout settings to comply with DHS policy.
4. Update FFMS password configuration settings to comply with DHS policy.
5. Train physical security personnel to recognize DHS issued identification and to deter non-conforming credentials.

Segregation of Duties:

1. Enforce policies and procedures to ensure that assigned roles and responsibilities are commensurate with personnel job functions.

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

Cause\Effect:

The ICE agency is not continuously monitoring the ICE ADEX General Support System (GSS) vulnerability assessment scans for patch and configuration management vulnerabilities. As a result, default configuration installations and unnecessary services operating on the ICE ADEX devices increase the ability to compromise the availability, integrity, and confidentiality of financial data on the network. Additionally, failure to apply critical vendor security patches exposes system and network devices to new and existing vulnerabilities. This can expose the information system controls environment to security breaches, unauthorized access, service interruptions, and denial of service attacks.

ICE management has not ensured that personnel are adequately trained and aware of the basic IT security policies described by DHS to ensure that system users are cognizant of computer security principles. Without proper training and awareness, system users could potentially provide unauthorized persons information to gain access to ICE resources and sensitive data that may result in loss, damage, or theft.

ICE management has not ensured that personnel are adequately trained and aware of the basic IT security policies described by DHS and ICE to protect their login credentials, lock network sessions to DHS systems, secure information system hardware, and securely store/limit access to FOUO and PII. The failure to control access to sensitive IT resources and ICE documentation could potentially result in the theft or destruction of ICE assets, unauthorized access to sensitive information, and disruptions in processing of ICE financial systems. Additionally, ICE personnel who are not adequately trained to protect their login credentials present an increased risk of unauthorized access to sensitive information from external and internal threats.

ICE personnel are not consistently complying with, or are unaware of, existing exit clearance procedures. By not having a more efficient process by which personnel are made aware of terminated or transferred employees, ICE's IT environment could be significantly impacted as these staff maintain unauthorized access or resources.

Due to lack of management oversight, background investigations are not initiated in a timely manner. By allowing personnel access to organization information and information systems without proper adjudication increases the risk of improper handling of sensitive information.

ICE management has not expended the time and resources necessary to formally document access review and recertification procedures for system user accounts and access privileges. Because access review and recertification procedures are not formally documented, reviewers do not have a standard for effectively conducting the recertification of FFMS accounts. This could lead to the risk of potentially allowing users to have account privileges that are no longer needed, or should not have been initially granted.

ICE management had not taken sufficient measures to ensure that financial system users comply with established policies related to the proper segregation of duties. Without enforcing compliance with proper segregation of duties, management is not able to maintain an effective control environment. The failure to segregate the initiation and approval of transactions on business applications results in an increased risk that transactions may be inappropriately executed.

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *Electronic Government Act of 2002*, mandates that Federal entities maintain IT security programs in accordance with OMB and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources*, and various NIST guidelines describe specific essential criteria for maintaining effective general IT controls. FFMIA sets forth legislation prescribing policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. The purpose of FFMIA is: (1) to provide for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government; (2) require Federal financial management systems to support full disclosure of Federal financial data, including the full costs of Federal programs and activities; (3) increase the accountability and credibility of federal financial management; (4) improve performance, productivity and efficiency of Federal Government financial management; and (5) establish financial management systems to support controlling the cost of Federal Government. In closing, for this year's IT audit we assessed the DHS component's compliance with DHS Sensitive System Policy Directive 4300A.

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

APPLICATION CONTROLs FINDINGS

We did not identify any findings in the area of application controls during the fiscal year 2009 ICE audit engagement.

MANAGEMENT’S COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from the Immigration and Customs Enforcement management. Generally, the ICE management agreed with all of our findings and recommendations. The ICE management has developed a remediation plan to address these findings and recommendations. We have included a copy of the comments in Appendix D.

OIG Response

We agree with the steps that ICE management is taking to satisfy these recommendations.

**Department of Homeland Security
Immigration and Customs Enforcement**
Information Technology Management Letter
September 30, 2009

Appendix A

**Description of Key ICE Financial Systems and IT Infrastructure
within the Scope of the FY 2009 DHS Financial Statement Audit**

**Department of Homeland Security
Immigration and Customs Enforcement**
Information Technology Management Letter
September 30, 2009

Below is a description of significant Immigration and Custom Enforcement (ICE) financial management systems and supporting information technology (IT) infrastructure included in the scope of ICE's fiscal year (FY) 2009 Financial Statement Audit.

Locations of Review: ICE Headquarters, Washington, DC; The Burlington Finance Center (BFC), Burlington, VT; Department of Commerce (DOC) Office of Computer Services (OCS), Springfield, VA.

Systems Subject to Audit:

- *Federal Financial Management System (FFMS):* It is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued. It is the system of record for the agency and supports all internal and external reporting requirements.
- *ICE Network:* The ICE Network, also know as the Active Directory/Exchange (ADEX) E-mail System, is the general support system (GSS) for ICE and other DHS components.

**Department of Homeland Security
Immigration and Customs Enforcement**
Information Technology Management Letter
September 30, 2009

Appendix B
FY 2009 Notices of IT Findings and Recommendations at ICE

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

Notice of Findings and Recommendations (NFR) – Definition of Severity Ratings:

Each NFR listed in Appendix B is assigned a severity rating from 1 to 3 indicating the influence on the Department of Homeland Security (DHS) Consolidated Independent Auditors Report.

1 – Not substantial

2 – Less significant

3 – More significant

The severity ratings indicate the degree to which the deficiency influenced the determination of severity for consolidated reporting purposes.

These rating are provided only to assist ICE in the development of its corrective action plans for remediation of the deficiency.

**Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009**

**FY 2009 Information Technology
Notification of Findings and Recommendations – Detail**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-09-11	We accessed ICE facilities located at the Tech World Building on 800 K Street and the PCN Tower on 500 and 12 th Street without the use of DHS issued credentials. Moreover, we overtly presented non-government issued identification to building security and was then granted physical access to the facilities.	We recommend that ICE train physical security personnel to recognize DHS issued identification or credentials and detect non-conforming credentials.	X		2
ICE-IT-09-12	Ineffective/non-compliant account lockout counter settings During the FY09 audit, KPMG inquired of ICE OCIO personnel about ADEX account settings, reviewed the account lockout settings, and inspected ICE's logical access policies and found that the account lockout settings for ADEX was not compliant with DHS policy. DHS policy requires that the system is to lock user accounts after three consecutive invalid login attempts within a 24 hour period. However, within ADEX, the number of invalid attempts to access the system resets to zero after 30 minutes if up to two invalid access attempts are made. Therefore, several attempts can initiated as long as the user waits 30 minutes before attempting again.	The Enterprise Operations Division of the OCIO adjusted the lockout settings after they were informed by us of the discrepancy. No recommendation given.	X		2
ICE-IT-09-13	We determined that the FFMS password settings require the use of an underscore and does not allow the use of any other special characters such as !, @, #, \$, %, or *, which is not compliant with DHS policy. The DHS policy requires that passwords contain a combination of alphabetic, numeric, and special characters.	We recommend that ICE update the FFMS password configuration settings to be in compliance with DHS 4300A policies.	X		2

Appendix B

**Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-09-14	We identified that the ADEX user recertification process is not designed appropriately. Specifically, we noted a lack of formal policy and procedure for managing the periodic review of ADEX general user access. In addition, the informal process contingent upon personnel's annual completion of the Information Assurance Awareness Training (IAAT) as a mitigating control for ensuring a review of users' access on a periodic basis is insufficient.	We recommend that ICE management establish and implement policies and procedures for recertification of ADEX user privileges. This process should include a method to document user recertification and a process to maintain evidence of the reviews.	X		2
ICE-IT-09-15	We inquired of ICE OCIO personnel about the process for recertifying FFMS user access (review of access privileges) and found that this process is not formally documented. Furthermore, we identified that the review for the access privileges for each FFMS account is not adequately recorded and no audit trail is available to support that a recertification was completed.	We recommend that ICE management establish and implement policies and procedures for recertification of FFMS user privileges. This process should include a method to document user recertification and a process to maintain evidence of the reviews.	X		2
ICE-IT-09-16	We determined that weaknesses exist over ADEX access. Specifically, we found that 14 users, which were separated from ICE, still had active ADEX accounts that were not removed upon their termination/transfer.	We recommend ICE management develop processes for the removal of transferred/terminated users within ADEX upon their separation.	X		2

Appendix B

**Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-09-17	We performed an inspection of a listing of FFMS users and their assigned roles/responsibilities and determined that 6 users had Originator, Funds Certification Official, and Approving Official profiles that were in violation of FFMS segregation of duties policies.	We recommend that ICE enforce policies and procedures to ensure that assigned roles and responsibilities are commensurate with personnel job functions.	X		2
ICE-IT-09-18	We identified that background reinvestigations are not conducted in a timely manner. We performed an inspection of a sample of ICE personnel requiring reinvestigations during the fiscal year and of the 25 ICE employees sampled, evidence of background reinvestigations during FY 2009 could not be provided for 16 contractors.	We recommend ICE management periodically review personnel files to confirm background reinvestigations have been completed in accordance with DHS standards.	X		2
ICE-IT-09-19	We performed an inspection of a sample of personnel that had terminated/transferred from their employment with ICE during the fiscal year. We requested evidence that exit clearance forms were completed for each employee to determine ICE management's compliance with exit clearance procedures. Of the 25 terminated/transferred ICE personnel sampled, evidence of compliance with exit clearance procedures could not be provided for 12 employees.	We recommend ICE management adhere to exit clearance procedures and require personnel to follow them in the event of transfer/termination.	X		2
ICE-IT-09-20	We determined that ICE lacks policies and procedures requiring completion of a training program by personnel in IT security positions.	We recommend that ICE management implement mandatory requirements for IT security personnel to complete training consistent with their job function duties.	X		2

Appendix B

**Department of Homeland Security
Immigration and Customs Enforcement**
Information Technology Management Letter
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-09-21	<p>During the internal vulnerability assessment efforts of ICE's network servers and systems we identified several High/ Medium Risk vulnerabilities, related to configuration management. We determined that security configuration management weaknesses (i.e., missing security patches and incorrect configuration settings) exist on hosts supporting the ICE.</p>	<p>In addition to addressing the specific vulnerabilities identified in the condition, ICE should:</p> <ul style="list-style-type: none"> • Redistribute procedures and train employees on continuously monitoring and mitigating vulnerabilities. In addition, we recommend that ICE periodically monitor the existence of unnecessary services and protocols running on their servers and network devices, in addition to deploying patches. • Perform vulnerability assessments and penetration tests on all offices of the ICE, from a centrally managed location with a standardized reporting mechanism that allows for trending, on a regularly scheduled basis in accordance with NIST guidance. • Develop a more thorough approach to track and mitigate configuration management vulnerabilities identified during monthly scans. ICE should monitor the vulnerability reports for necessary or required configuration changes to their environment. • Develop a process to verify that systems identified with "HIGH/MEDIUM Risk" configuration vulnerabilities do not appear on subsequent monthly vulnerability scan reports, unless they are verified and documented as a false-positive. All risks identified during the monthly scans should be 	X		2

Appendix B

**Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-09-22	During our after hours physical testing, we identified 26 passwords, 4 For Official Use Only Violations , 2 unsecured ID badges/keys, 15 Personally Identifiable Information violations, 2 server names/IP addresses, 3 unsecured laptops, 6 unsecured external drives, 1 unsecured credit card, and 2 users logged into a system without an active screen saver set.	mitigated immediately, and not be allowed to remain dormant. KPMG recommends that ICE management implement processes to: <ul style="list-style-type: none"> • Ensure that users are trained and aware of safeguarding login credentials, locking network sessions to DHS systems, and locking any sensitive information, media containing sensitive information, or data not suitable for public dissemination in secure locations when not in use. • Effectively limit access to DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data to authorized personnel 	X		2
ICE-IT-09-23	We identified that the IT security awareness training requirements are not enforced. Of the population of staff that had not taken the training by the ICE deadline of 6/1/09, we determined that 3 employees still maintained system access. Additionally, procedures are not in place to disable user accounts and access privileges if annual training is not completed.	We recommend ICE management to: <ul style="list-style-type: none"> • Remove system access for personnel that are not in compliance with training requirements. • Document procedures regarding the disabling of user accounts and access privileges in accordance with DHS policies for employees not in compliance. 	X		2

**Department of Homeland Security
Immigration and Customs Enforcement**
Information Technology Management Letter
September 30, 2009

APPENDIX C

**Status of Prior Year Notices of Findings and Recommendations
and Comparison to
Current Year Notices of Findings and Recommendations at ICE**

**Department of Homeland Security
Immigration and Customs Enforcement**
Information Technology Management Letter
September 30, 2009

		Disposition	
NFR No.	Description	Closed	Repeat
ICE-IT-08-04	Weak ICE Network/ADEX Access Controls Exist	X	
ICE-IT-08-09	ICENet/ADEX Contingency Plan is not Stored at Offsite Locations	X	
ICE-IT-08-10	ICENet/ADEX Backup Facility Access is not Appropriately Secured from Unauthorized Access	X	

Department of Homeland Security
Immigration and Customs Enforcement
Information Technology Management Letter
September 30, 2009

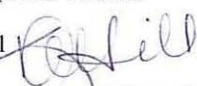
Office of the Assistant Secretary
U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20536



**U.S. Immigration
and Customs
Enforcement**

March 18, 2010

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Information Technology
Office of Inspector General

FROM: Kathy A. Hill 
Director
Office of Assurance and Compliance

SUBJECT: Response to the DHS Office of Inspector General Draft Report:
"Information Technology Management Letter for the FY 2009 ICE
Financial Integrated Audit" dated February 18, 2009

Thank you for the opportunity to comment on the above subject draft report. The U.S. Immigration and Customs Enforcement (ICE) is committed to ensuring the proper internal controls are in place to safeguard critical financial and operational data.

ICE concurred with all 13 of the recommendations contained in the draft report. Recommendations ICE-IT-09-11 and ICE-IT-09-18 have been assigned to the Office of Professional Responsibility, ICE-IT-09-19 has been assigned to the Office of Human Capital, and the Office of the Chief Financial Officer will monitor these recommendations. Previously, we requested that these recommendations be resolved and closed. The remaining 10 recommendations will be resolved by the Office of the Chief Information Officer. Corrective actions for these 10 recommendations are contained in the Trusted Agent FISMA (TAF).

Should you have any questions or concerns, please contact Claude Lucas, senior audit portfolio manager at (202) 732-4162 or by e-mail at Claude.Lucas@dhs.gov.

**Department of Homeland Security
Immigration and Customs Enforcement**
Information Technology Management Letter
September 30, 2009

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Assistant Secretary, ICE
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, ICE
Chief Information Officer, ICE
Chief Information Security Officer
Assistant Secretary, Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison
ICE Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees as Appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.